BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC CHUYỂN ĐỔI SỐ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 231 /QĐ-CĐS

Hà Nội, ngày 13 tháng 11 năm 2026

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an ninh mạng Cục Chuyển đổi số

CỤC TRƯỞNG CỤC CHUYỂN ĐỔI SỐ

Căn cứ Luật Dữ liệu ngày 30 tháng 11 năm 2024;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26 tháng 6 năm 2025;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 10 tháng 12 năm 2025;

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ Quy chuẩn kỹ thuật quốc gia QCVN 12:2026/BCA An ninh mạng cho hệ thống thông tin lưu trữ tài liệu điện tử trong các cơ quan đảng, Nhà nước;

Căn cứ Tiêu chuẩn quốc gia TCVN 14423:2026 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng;

Căn cứ Quyết định số 223/QĐ-BNNMT ngày 01 tháng 3 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Chuyển đổi số;

Căn cứ Quyết định số 3785/QĐ-BNNMT ngày 05 tháng 10 năm 2026 của Bộ trưởng Bộ Nông nghiệp và Môi trường ban hành Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường;

Theo đề nghị của Trưởng phòng An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng Cục Chuyển đổi số.

Điều 2. Quyết định này có hiệu lực từ ngày ký và thay thế cho Quyết định số 114/QĐ-CĐS ngày 14 tháng 7 năm 2025 của Cục trưởng Cục Chuyển đổi số ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Chuyển đổi số.

Điều 3. Chánh Văn phòng Cục; Trưởng phòng An toàn thông tin; lãnh đạo các đơn vị thuộc Cục; công chức, viên chức, người lao động thuộc Cục Chuyển đổi số và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thứ trưởng Đặng Ngọc Điệp (để báo cáo);
- Các Phó Cục trưởng (để chỉ đạo);
- Các đơn vị trực thuộc Bộ (để phối hợp);
- Các đơn vị thuộc Cục (để thực hiện);
- Lưu: VT, ATTT.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CHUYỂN ĐỔI SỐ
BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Lê Phú Hà

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC CHUYỂN ĐỔI SỐ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY CHẾ
BẢO ĐẢM AN NINH MẠNG CỤC CHUYỂN ĐỔI SỐ

(Kèm theo Quyết định số /QĐ-CĐS ngày tháng năm 2026 của Cục trưởng Cục Chuyển đổi số)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh, đối tượng áp dụng

1. Phạm vi điều chỉnh: Quy chế này quy định bảo đảm an ninh mạng trong các hoạt động của Cục Chuyển đổi số (sau đây viết tắt là Cục).

2. Đối tượng áp dụng

a) Các đơn vị thuộc Cục Chuyển đổi số (sau đây viết tắt là đơn vị thuộc Cục) và công chức, viên chức, người lao động thuộc các đơn vị thuộc Cục.

b) Cơ quan, tổ chức, cá nhân sử dụng dịch vụ công nghệ thông tin, an ninh mạng tại Trung tâm dữ liệu của Bộ do Cục quản lý.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin, an ninh mạng cho các đơn vị thuộc Cục.

Điều 2. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. An ninh mạng là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

2. An ninh dữ liệu là sự bảo đảm chất lượng dữ liệu và các hoạt động xử lý, sử dụng dữ liệu trên không gian mạng phục vụ phát triển kinh tế - xã hội, chuyển đổi số quốc gia, tránh bị truy cập, sử dụng, tiết lộ, sửa đổi trái phép, phá hoại hoặc hành vi khác đe dọa hoặc gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội.

3. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. Hạ tầng kỹ thuật là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng…

5. Cổng thông tin điện tử là điểm truy cập duy nhất của cơ quan, đơn vị trên môi trường mạng, liên kết, tích hợp các kênh thông tin, các dịch vụ và các ứng dụng

mà qua đó người dùng có thể khai thác, sử dụng và cá nhân hóa việc hiển thị thông tin.

6. Trang thông tin điện tử là hệ thống thông tin dùng để thiết lập một hoặc nhiều trang thông tin được trình bày dưới dạng ký hiệu, số, chữ viết, hình ảnh, âm thanh và các dạng thông tin khác phục vụ cho việc cung cấp và sử dụng thông tin trên Internet.

7. Mạng là một hệ thống kết nối nhiều thiết bị với nhau (như máy tính, điện thoại, máy in, máy chủ…) nhằm mục đích chia sẻ dữ liệu, tài nguyên và thông tin.

8. Chủ quản hệ thống thông tin là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với hệ thống thông tin.

9. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

10. Sự cố an ninh mạng là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

11. Rủi ro an ninh mạng là khả năng bị lộ hoặc mất mát do một cuộc tấn công mạng hoặc vi phạm dữ liệu trong cơ quan, tổ chức, đơn vị. Rủi ro an ninh mạng không chỉ nằm ở khả năng xảy ra một cuộc tấn công mạng mà còn là những hậu quả tiềm ẩn, ví dụ như tổn thất tài chính, thiệt hại về danh tiếng hoặc gián đoạn hoạt động.

12. Thiết bị số là thiết bị điện tử, máy tính, viễn thông, truyền dẫn, thu phát sóng vô tuyến điện và thiết bị tích hợp khác được sử dụng để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin số.

13. Trung tâm dữ liệu/phòng máy chủ là một tòa nhà, không gian dành riêng trong tòa nhà hoặc một nhóm các tòa nhà được sử dụng để đặt tập trung hệ thống máy chủ, thiết bị lưu trữ, thiết bị định tuyến, thiết bị chuyển mạch, thiết bị bảo đảm an ninh mạng, thiết bị ngoại vi, đường truyền kết nối Internet, nguồn điện dự phòng, hệ thống làm lạnh, thiết bị phòng cháy, chữa cháy, chống sét, thiết bị hỗ trợ và các trang thiết bị khác.

Điều 3. Nguyên tắc bảo đảm an ninh mạng

Thực hiện theo Điều 4 Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường tại Quyết định số 3785/QĐ-BNNMT ngày 05 tháng 10 năm 2026 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc ban hành Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 4. Các hành vi bị nghiêm cấm

Thực hiện theo Điều 3 Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường tại Quyết định số 3785/QĐ-BNNMT ngày 05 tháng 10 năm 2026 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc ban hành Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường.

Chương II
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG ĐỐI VỚI HẠ TẦNG CÔNG NGHỆ THÔNG TIN DÙNG CHUNG CỦA BỘ

Điều 5. Quản lý an ninh mạng đối với Trung tâm dữ liệu

1. Trung tâm dữ liệu là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định của thủ trưởng cơ quan, đơn vị mới được phép vào Trung tâm dữ liệu. Quá trình vào, ra phải được ghi nhận vào nhật ký quản lý Trung tâm dữ liệu.

2. Phải có hệ thống giám sát và bảo đảm an toàn phù hợp với yêu cầu của từng cấp độ an toàn theo quy định tại Phụ lục A – Tiêu chuẩn quốc gia TCVN 14423:2026.

3. Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như tường lửa, thiết bị định tuyến, hệ thống máy chủ, hệ thống lưu trữ… phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy nhập, kết nối vật lý phù hợp với từng khu vực: máy chủ và hệ thống lưu trữ; tủ mạng và đầu nối; thiết bị nguồn điện và dự phòng điện khẩn cấp; vận hành, kiểm soát, quản trị hệ thống.

4. Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ để duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về độ sẵn sàng trong suốt thời gian vận hành.

5. Các đơn vị được giao quản trị, vận hành Trung tâm dữ liệu có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc tại khu vực này; cử cán bộ thường xuyên giám sát thiết bị, hạ tầng của Trung tâm dữ liệu.

Điều 6. Quản lý an ninh mạng đối với hệ thống máy chủ và ứng dụng đặt tại Trung tâm dữ liệu

1. Hệ thống máy chủ phải được đặt trong các vùng mạng dành riêng cho máy chủ, tối thiểu gồm vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ, vùng mạng máy chủ cơ sở dữ liệu và vùng quản trị.

2. Chỉ cài đặt và sử dụng các phần mềm có bản quyền, nguồn gốc rõ ràng, thực sự cần thiết. Không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ cập nhật bản vá bảo mật khi không thực sự cần thiết.

3. Cài đặt các giải pháp phòng chống mã độc tập trung và phòng chống tấn công xâm nhập mạng phù hợp với yêu cầu theo từng cấp độ.

4. Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố. Đối với các hệ thống thông tin cần thực hiện quy tắc sao lưu dự phòng 3-2-1: có 03 bản sao lưu dự phòng; lưu trữ ít nhất trên 02 loại phương tiện khác nhau; 01 bản được lưu trữ offline. Định kỳ kiểm tra tính toàn vẹn và khả năng khôi phục thành công hệ thống từ các bản sao lưu.

5. Giám sát thường xuyên, liên tục các máy chủ, đặc biệt là các truy cập đến máy chủ cung cấp dịch vụ nền tảng như vCenter, ESXi, Domain Controller… để phát hiện và cảnh báo sớm nguy cơ mất an toàn an ninh mạng.

6. Định kỳ tìm kiếm, đánh giá, điều tra các dấu hiệu tấn công mạng, rà quét mã độc trên toàn bộ hệ thống. Thông báo và phối hợp với các đầu mối ứng cứu sự cố an ninh mạng của Cục để xử lý nếu phát hiện thấy bất thường trong hệ thống.

7. Các hệ thống thông tin, phần mềm ứng dụng, dịch vụ cài đặt trên máy chủ

a) Không được cài các phần mềm điều khiển máy tính từ xa của bên thứ ba như TeamViewer, AnyDesk, UltraViewer…

b) Hệ thống thông tin, phần mềm ứng dụng phải đáp ứng các yêu cầu sau: cấu hình để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị hệ thống thông tin, phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

d) Ghi và lưu giữ bản ghi nhật ký hệ thống của hệ thống thông tin, phần mềm ứng dụng trong khoảng thời gian tối thiểu 12 tháng với những thông tin cơ bản: thời gian, địa chỉ kết nối, tài khoản (nếu có), nội dung truy cập dữ liệu, dịch vụ; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị, thông tin thay đổi cấu hình máy chủ.

đ) Cần được kiểm tra phát hiện và khắc phục các điểm yếu về an ninh mạng trước khi đưa vào sử dụng và trong quá trình sử dụng. Định kỳ thực hiện quy trình kiểm soát cài đặt, cập nhật, vá các điểm yếu bảo mật của hệ thống thông tin, phần mềm ứng dụng, dịch vụ trên các máy chủ.

Điều 7. Quản lý an ninh mạng khi xây dựng, tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

1. Khi thực hiện xây dựng, nâng cấp, mở rộng, thay thế một phần hệ thống thông tin, phải xây dựng hoặc rà soát cấp độ, phương án bảo đảm an ninh mạng của hệ thống thông tin và thực hiện điều chỉnh, bổ sung hoặc thay mới hồ sơ đề xuất cấp độ trong trường hợp cần thiết.

2. Khi xây dựng, tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, đơn vị phải tiến hành phân tích, xác định rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

3. Các hệ thống thông tin cài đặt tại Trung tâm dữ liệu của Bộ phải tách biệt với các môi trường phát triển, kiểm tra và thử nghiệm. Các vùng mạng này không được kết nối ra ngoài Internet. Nếu quá trình thử nghiệm bắt buộc phải có kết nối ra ngoài Internet thì phải đăng ký với đơn vị chuyên trách về an ninh mạng của Cục để thiết lập chỉ cho phép kết nối đến đúng địa chỉ IP, đường dẫn URL (Uniform Resource Locator), các cổng kết nối cần thiết trong khoảng thời gian cho phép.

4. Trong quá trình vận hành hệ thống thông tin, đơn vị chủ quản hệ thống thông tin cần thực hiện đánh giá, phân loại hệ thống thông tin theo cấp độ; triển khai phương án bảo đảm an ninh mạng đối với hệ thống thông tin đáp ứng yêu cầu cơ bản trong tiêu chuẩn, quy chuẩn kỹ thuật về bảo đảm an ninh mạng hệ thống thông tin theo cấp độ; thường xuyên kiểm tra, giám sát an ninh mạng đối với hệ thống thông tin; tuân thủ quy trình vận hành, quy trình xử lý sự cố đã xây dựng; ghi lại và lưu trữ đầy đủ thông tin nhật ký hệ thống để phục vụ quản lý, kiểm soát thông tin.

5. Các đơn vị thuộc Cục liên quan đến việc phát triển phần mềm ứng dụng có trách nhiệm yêu cầu các đối tác (nếu có) thực hiện các công tác bảo đảm an ninh mạng, tránh lộ, lọt mã nguồn và dữ liệu, tài liệu thiết kế, quản trị hệ thống mà đối tác đang xử lý ra bên ngoài.

Chương III
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG NỘI BỘ DO CỤC QUẢN LÝ

Điều 8. Quản lý an ninh mạng đối với hệ thống mạng nội bộ

1. Phải được thiết kế phân vùng theo chức năng cơ bản (theo các chính sách an ninh mạng riêng), bao gồm nhưng không giới hạn các vùng mạng sau: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị.

2. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị bảo mật và giám sát an ninh mạng.

3. Thiết lập, cấu hình các tính năng theo thiết kế của các trang thiết bị bảo mật mạng; thực hiện các biện pháp, giải pháp để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng về mặt kỹ thuật của hệ thống mạng; thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng.

4. Thiết lập cấu hình chỉ cho phép kết nối mạng nội bộ sau khi các máy tính phục vụ công việc được đăng ký thông tin địa chỉ mạng vật lý (địa chỉ MAC).

5. Định kỳ sao lưu cấu hình thiết bị kết nối mạng nội bộ. Lưu trữ tối thiểu trong 12 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam.

6. Định kỳ thực hiện kiểm soát các phần mềm cài đặt, cập nhật, vá lỗi các điểm yếu bảo mật phần mềm, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

7. Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây cáp mạng phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối các cổng mạng không sử dụng.

8. Không được tiết lộ thiết kế, thông số cấu hình hệ thống mạng nội bộ cho tổ chức, cá nhân khác khi chưa được các cấp có thẩm quyền cho phép; không được tìm cách truy cập dưới bất cứ hình thức nào vào các khu vực không được phép truy cập.

Điều 9. Quản lý an ninh mạng đối với kết nối Internet

Hệ thống mạng của Cục phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an ninh mạng trong kết nối vào Internet, tối thiểu đáp ứng các yêu cầu sau:

1. Có hệ thống tường lửa và hệ thống bảo vệ truy cập Internet, đáp ứng nhu cầu kết nối đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ.

2. Thiết lập mạng không dây riêng tách biệt với mạng nội bộ phục vụ cho các đối tác và người dùng vào mạng Internet. Mật khẩu kết nối mạng không dây phải được thay đổi định kỳ tối thiểu 01 năm/lần, độ phức tạp trên 08 ký tự bao gồm tối thiểu 4 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (' ~ ! @ # $ % ^ & * () _ - + = { } [ ] \ I : ; “ ‘ <> , . ? /).

3. Lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc; hoạt động đánh bạc, lừa đảo trực tuyến; tuyên truyền phản động hoặc các nội dung không phù hợp khác.

4. Các đơn vị và cá nhân tham gia vào hệ thống mạng máy tính không được tự ý thay đổi những thông số mạng hay tự ý đưa các thiết bị mạng, thiết bị viễn thông khác tham gia kết nối vào hệ thống mạng.

Điều 10. Quản lý an ninh mạng đối với tài khoản truy cập

1. Tài khoản truy cập (gọi tắt là tài khoản) là tập hợp gồm tên đăng nhập và mật khẩu hoặc/và hình thức xác thực khác, được gắn với quyền truy cập thực hiện một số tác vụ trên hệ thống thông tin hoặc trên thiết bị xử lý thông tin do Cục quản lý; bao gồm các loại sau:

a) Tài khoản truy cập hệ thống gắn với một nhiệm vụ cụ thể, được gắn với quyền truy cập thực hiện các tác vụ cần thiết cho nhiệm vụ đó (ví dụ: tài khoản văn thư, tài khoản biên tập…).

b) Tài khoản quản trị gắn với quyền cài đặt, cấu hình các thông số và cấp quyền truy cập trên hệ thống thông tin, gồm: quản trị nội dung, quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị.

2. Tài khoản quản trị được giao cho cá nhân, đơn vị thực hiện nhiệm vụ quản trị ứng dụng, quản trị cơ sở dữ liệu, quản trị hệ điều hành, quản trị thiết bị, Trung tâm Hạ tầng số giữ ít nhất 01 tài khoản quản trị hệ điều hành của tất cả các máy chủ hoạt động trong mạng nội bộ Cục.

3. Quy định về mật khẩu của tài khoản truy cập:

a) Mật khẩu tài khoản truy cập hệ thống cho người dùng phải đáp ứng các yêu cầu: có tối thiểu 10 ký tự, gồm tối thiểu 3 trong 4 loại ký tự sau: chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 - 9), các ký tự khác trên bàn phím máy tính (` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ I : ; " ' < > , . ? /) và dấu cách; không chứa tên tài khoản; mật khẩu phải được thay đổi tối thiểu 12 tháng một lần.

b) Mật khẩu tài khoản quản trị phải đáp ứng các yêu cầu: có tối thiểu 15 ký tự, gồm tối thiểu 3 trong 5 loại ký tự sau: chữ cái viết hoa (A - Z); chữ cái viết thường (a - z); chữ số (0 - 9); các ký tự khác trên bàn phím máy tính (' ~ ! @ # $ % ^ & * () _ - + = { } [ ] \ I : ; “ ‘ <> , . ? /) và dấu cách; không chứa tên tài khoản; mật khẩu phải được thay đổi tối thiểu 02 tháng một lần.

4. Cá nhân được cấp hoặc giao tài khoản chịu trách nhiệm về các hành vi của tài khoản được ghi nhận trên thiết bị xử lý thông tin, hệ thống thông tin, hệ thống giám sát an ninh mạng.

5. Đơn vị vận hành hệ thống thông tin thường xuyên rà soát các tài khoản truy cập hệ thống đang hoạt động, phát hiện và thu hồi các tài khoản không sử dụng hoặc không hợp lệ, điều chỉnh thông tin tài khoản chưa phản ánh chính xác thông tin thực tế tại thời điểm rà soát.

Điều 11. Quản lý an ninh mạng đối với dữ liệu

Thực hiện theo Điều 13 Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường tại Quyết định số 3785/QĐ-BNNMT ngày 05 tháng 10 năm 2026 của Bộ trưởng Bộ Nông nghiệp và Môi trường ban hành Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 12. Quản lý an ninh mạng đối với thiết bị số

1. Thiết bị số phục vụ quản trị hệ thống:

a) Phải cài đặt các phần mềm bảo đảm an ninh mạng do Cục cung cấp, bao gồm nhưng không giới hạn: phần mềm chống mã độc tập trung, công cụ kết nối VPN.

b) Chỉ cài đặt và sử dụng các phần mềm quản trị đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết.

2. Thiết bị số của các đơn vị thuộc Cục kết nối vào mạng nội bộ phải đáp ứng đầy đủ các yêu cầu sau:

a) Phải đăng ký với đơn vị chuyên trách an ninh mạng của Cục các địa chỉ mạng vật lý (MAC).

b) Sử dụng hệ điều hành được hỗ trợ bản vá lỗ hổng bảo mật. Chỉ cài đặt tiện ích thiết yếu được cung cấp kèm theo hệ điều hành và các phần mềm phục vụ công việc, có bản quyền hoặc được các cơ quan chức năng đánh giá, xác nhận an toàn. Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về an toàn thông tin mạng để được xử lý kịp thời.

3. Thiết bị số soạn thảo văn bản chứa nội dung bí mật nhà nước, lưu trữ bí mật nhà nước:

a) Sử dụng hệ điều hành và các phần mềm soạn thảo văn bản có bản quyền. Không kết nối vào mạng Internet, mạng nội bộ, mạng không dây, mạng viễn thông.

b) Trường hợp thiết bị lưu trữ lỗi cần mang đi bảo hành, phải thực hiện biện pháp xóa dữ liệu vĩnh viễn trước khi mang ra khỏi cơ quan và có biên bản ghi nhận

về việc xóa dữ liệu giữa đơn vị sử dụng máy tính và đơn vị nhận thiết bị lưu trữ. Việc sửa chữa, nâng cấp phần mềm cho máy tính (sau khi đã đưa vào sử dụng), nếu yêu cầu phải tiếp cận các tệp tin trên thiết bị lưu trữ, phải thực hiện dưới sự giám sát của đơn vị sử dụng thiết bị số, bảo đảm không lộ lọt dữ liệu trên thiết bị lưu trữ ra bên ngoài trong quá trình này (có biên bản giữa đơn vị sử dụng thiết bị số và đơn vị sửa chữa, nâng cấp phần mềm).

4. Thiết bị lưu trữ di động cho các hoạt động nghiệp vụ, quản lý chỉ được sử dụng khi thực hiện các biện pháp bảo đảm an ninh, an toàn cho thiết bị như mã hóa dữ liệu, quét mã độc định kỳ.

Điều 13. Quy định đối với cán bộ, công chức, viên chức và người lao động tham gia công tác bảo đảm an ninh mạng

1. Điều kiện, yêu cầu của nhân sự làm công tác quản trị mạng, vận hành hệ thống, bảo đảm an ninh mạng

a) Có phẩm chất đạo đức tốt, có đủ tiêu chuẩn chính trị, có kiến thức pháp luật và chuyên môn, nghiệp vụ về bảo vệ thông tin bí mật, nghiêm chỉnh chấp hành đường lối, chủ trương, chính sách của Đảng, pháp luật của Nhà nước.

b) Có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an ninh mạng, phù hợp với vị trí tuyển dụng.

c) Đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, nhân sự phải có cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động, bao gồm các điều khoản về trách nhiệm của cá nhân trong quá trình công tác và sau khi thôi việc tại đơn vị.

2. Khi cán bộ, công chức, viên chức và người lao động chấm dứt hoặc thay đổi công việc, các đơn vị phải:

a) Lập biên bản bàn giao tài sản công nghệ thông tin với đơn vị chủ quản và các đơn vị liên quan.

b) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

c) Rà soát, kiểm tra đối chiếu định kỳ giữa bộ phận quản lý nhân sự và bộ phận quản lý cấp phát, thu hồi quyền truy cập hệ thống thông tin để bảo đảm tài khoản người dùng của công chức, viên chức và người lao động đã nghỉ việc được thu hồi.

Điều 14. Giám sát, kiểm tra, đánh giá an ninh mạng

1. Giao Trung tâm Hạ tầng số chủ trì, phối hợp với các đơn vị thực hiện giám sát an ninh mạng cho toàn bộ hạ tầng công nghệ thông tin dùng chung của Bộ, mạng nội bộ và mạng không dây do Cục quản lý.

2. Trung tâm Hạ tầng số có trách nhiệm giám sát và cấu hình cảnh báo các thay đổi trên các hệ thống; các hành vi cố gắng truy cập, đăng nhập thành công hoặc không thành công vào các hạ tầng quan trọng như hạ tầng ảo hóa, Domain Controller, VPN…

3. Trung tâm Hạ tầng số có trách nhiệm thông báo cho các đầu mối ứng cứu sự cố của Cục và đơn vị vận hành hệ thống thông tin khi phát hiện hệ thống thông tin đang bị tấn công mạng; ngắt kết nối mạng hoặc tắt máy chủ, máy trạm đang bị lây nhiễm mã độc để hạn chế thiệt hại và mất mát thông tin, dữ liệu.

4. Phòng An toàn thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an ninh mạng đối với hệ thống thông tin theo cấp độ. Nội dung kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về an ninh mạng đối với hệ thống thông tin theo cấp độ theo quy định tại khoản 1 Điều 27 của Nghị định số 331/2026/NĐ-CP.

5. Phòng An toàn thông tin phối hợp với Trung tâm Hạ tầng số thực hiện việc đánh giá hiệu quả các biện pháp bảo đảm an ninh mạng theo phương án bảo đảm an ninh mạng được phê duyệt. Nội dung kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng theo phương án bảo đảm an ninh mạng được phê duyệt theo quy định tại khoản 2 Điều 27 của Nghị định 331/2026/NĐ-CP.

6. Nội dung kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin; hình thức kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin theo quy định tại khoản 3 và khoản 4 Điều 27 của Nghị định 331/2026/NĐ-CP.

Điều 15. Quy định về bảo vệ dữ liệu cá nhân

1. Nguyên tắc bảo vệ dữ liệu cá nhân:

a) Việc thu thập, lưu trữ, xử lý, chia sẻ và xóa dữ liệu cá nhân tại Cục phải tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân, pháp luật về lưu trữ và Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường ban hành kèm Quyết định 3785/QĐ-BNNMT của Bộ trưởng Bộ Nông nghiệp và Môi trường.

b) Dữ liệu cá nhân được thu thập và xử lý phải đúng mục đích, trong phạm vi chức năng, nhiệm vụ, quyền hạn được giao; tuyệt đối không sử dụng vào mục đích khác hoặc chia sẻ trái phép cho bên thứ ba.

2. Trách nhiệm của các đơn vị, công chức, viên chức và người lao động thuộc Cục:

a) Phòng An toàn thông tin là đơn vị chuyên trách bảo vệ dữ liệu cá nhân thuộc Cục; chủ trì tham mưu, triển khai các biện pháp bảo đảm an toàn dữ liệu cá nhân, xây dựng và cập nhật Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân của Cục (nếu có); làm đầu mối phối hợp với các cơ quan quản lý chuyên ngành thuộc Bộ, với Bộ Công an trong công tác bảo vệ dữ liệu cá nhân theo Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường ban hành kèm Quyết định 3785/QĐ-BNNMT của Bộ trưởng Bộ Nông nghiệp và Môi trường.

b) Các đơn vị thuộc Cục: Tổ chức thu thập, xử lý dữ liệu cá nhân của tổ chức, cá nhân theo thẩm quyền, chức năng, nhiệm vụ được giao; quản lý dữ liệu cá nhân của công chức, viên chức, người lao động thuộc phạm vi quản lý đơn vị theo đúng

quy trình, quy định của pháp luật về bảo vệ dữ liệu cá nhân; bảo đảm có sự đồng ý của chủ thể dữ liệu (trừ trường hợp cơ quan nhà nước xử lý dữ liệu phục vụ hoạt động của cơ quan theo quy định của pháp luật); thực hiện các quy định về bảo vệ dữ liệu cá nhân tại Chương III Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường ban hành kèm Quyết định 3785/QĐ-BNNMT của Bộ trưởng Bộ Nông nghiệp và Môi trường.

c) Cán bộ, công chức, viên chức, người lao động: Tuân thủ quy định bảo mật thông tin trong thực thi công vụ; không tự ý sao chép, trích xuất, chuyển giao dữ liệu cá nhân ra khỏi hệ thống quản lý của đơn vị trái quy định; nghiêm chỉnh tuân thủ các quy định về bảo vệ dữ liệu cá nhân tại Chương III Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường ban hành kèm Quyết định 3785/QĐ-BNNMT của Bộ trưởng Bộ Nông nghiệp và Môi trường.

3. Kết nối, chia sẻ dữ liệu cá nhân giữa các cơ quan nhà nước:

a) Việc chia sẻ dữ liệu cá nhân với các cơ quan nhà nước khác phải được thực hiện thông qua Nền tảng tích hợp, chia sẻ dữ liệu cấp Bộ/tỉnh (LGSP) và kết nối với Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NDXP); không thực hiện chia sẻ qua các kênh không bảo mật hoặc chưa được mã hóa.

b) Các đơn vị chỉ thực hiện chia sẻ dữ liệu đúng mục đích thực thi công vụ và không xâm phạm quyền lợi hợp pháp của chủ thể dữ liệu.

c) Trung tâm Hạ tầng số có trách nhiệm áp dụng các biện pháp kỹ thuật để kiểm soát, giám sát, ghi nhật ký (log) luồng dữ liệu chia sẻ; kịp thời phát hiện và ngăn chặn các truy cập, kết nối trái phép vượt quá thẩm quyền quy định; nhật ký (log) kết nối, chia sẻ được lưu trữ tối thiểu 02 năm.

4. Khai thác, sử dụng thông tin từ Cơ sở dữ liệu quốc gia về Dân cư:

a) Việc kết nối, khai thác thông tin từ Cơ sở dữ liệu quốc gia về Dân cư chỉ được thực hiện thông qua tài khoản công vụ, thiết bị, hệ thống đã được Bộ Công an kiểm tra, xác nhận đủ điều kiện về an ninh, an toàn thông tin và cấp phép.

b) Chỉ kết nối, truy vấn thông tin cá nhân phục vụ trực tiếp cho việc giải quyết thủ tục hành chính hoặc thực hiện nhiệm vụ công vụ cụ thể được giao.

c) Đơn vị vận hành hệ thống có kết nối Cơ sở dữ liệu quốc gia về Dân cư có trách nhiệm lưu trữ lịch sử truy cập (log hệ thống) của từng tài khoản công vụ tối thiểu 02 năm để phục vụ công tác thanh tra, kiểm tra an ninh khi có yêu cầu từ Bộ Công an hoặc cơ quan có thẩm quyền.

5. Tiếp nhận, giải quyết yêu cầu và xử lý sự cố an ninh dữ liệu:

a) Tiếp nhận và giải quyết kịp thời các quyền của chủ thể dữ liệu (cung cấp, đính chính, xóa dữ liệu) theo đúng quy trình, quy chế của đơn vị quản lý dữ liệu, quy định của pháp luật về bảo vệ dữ liệu cá nhân, pháp luật về lưu trữ.

b) Khi phát hiện hành vi vi phạm hoặc sự cố mất an toàn, rò rỉ dữ liệu cá nhân (bao gồm cả dữ liệu trong quá trình kết nối, chia sẻ và khai thác thông tin dân cư), các đơn vị, cá nhân phải có trách nhiệm báo cáo ngay về Phòng An toàn thông tin để phối hợp cô lập, khắc phục và xử lý theo quy định tại Điều 29 Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 16. Ứng cứu sự cố an ninh mạng

1. Phòng An toàn thông tin và Trung tâm Hạ tầng số có trách nhiệm theo dõi, nắm bắt thông tin trên phương tiện thông tin đại chúng và mạng Internet về các sự kiện mất an ninh mạng có thể tác động tới đơn vị; chủ động kiểm tra, rà soát theo các văn bản cảnh báo, hướng dẫn của các cơ quan chức năng và các tổ chức về an ninh mạng; thiết lập kênh trao đổi thông tin với các đối tác cung cấp thiết bị, phần mềm, giải pháp an ninh mạng của đơn vị để nắm bắt kịp thời vấn đề, sự cố có khả năng tác động tới hệ thống thông tin.

2. Các đơn vị vận hành rà soát, đánh giá các rủi ro và sự cố an ninh mạng (phân loại theo sự cố thông thường và sự cố nghiêm trọng) có thể xảy ra để xây dựng, trình Cục phê duyệt phương án và quy trình ứng cứu sự cố cho hệ thống thông tin trong phạm vi quản lý.

3. Khi phát hiện sự cố an ninh mạng thuộc loại hình tấn công mạng, đơn vị vận hành hệ thống thông tin phải thông báo tới Phòng An toàn thông tin, Trung tâm Hạ tầng số để cùng phối hợp điều tra và khắc phục sự cố.

4. Quy trình ứng cứu sự cố an ninh mạng được thực hiện theo khoản 3 Điều 18 Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường tại Quyết định số 3785/QĐ-BNNMT ngày 05 tháng 10 năm 2026 của Bộ trưởng Bộ Nông nghiệp và Môi trường ban hành Quy chế bảo đảm an ninh mạng Bộ Nông nghiệp và Môi trường.

5. Các đơn vị cử cán bộ tham gia đầy đủ các cuộc diễn tập về ứng cứu sự cố an ninh mạng do Cục tổ chức.

6. Các đơn vị vận hành hệ thống thông tin cử 01 lãnh đạo đơn vị và ít nhất 01 chuyên viên làm đầu mối ứng cứu sự cố để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Phòng An toàn thông tin, Trung tâm Hạ tầng số trong các hoạt động giám sát an ninh mạng tại đơn vị và tại Cục.

Điều 17. Phổ biến, tuyên truyền, đào tạo, bồi dưỡng về an ninh mạng

1. Phòng An toàn thông tin phối hợp với Văn phòng Cục và các đơn vị liên quan lập kế hoạch và triển khai công tác tuyên truyền, phổ biến chủ trương, chính sách, pháp luật, biện pháp an ninh mạng, thông qua các hình thức: văn bản, gửi thư điện tử và các hình thức khác phù hợp với quy định của pháp luật. Các đơn vị thuộc Cục có trách nhiệm thực hiện quán triệt, tuyên truyền, phổ biến, nâng cao nhận thức, trách nhiệm về an ninh mạng cho cán bộ, công chức, viên chức, người lao động thuộc đơn vị.

2. Phòng An toàn thông tin phối hợp với Trung tâm Hạ tầng số tổ chức đào tạo, bồi dưỡng theo các chương trình đào tạo ngắn hạn nâng cao kiến thức, kỹ năng về an ninh mạng cho công chức, viên chức, người lao động.

Chương IV
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN LIÊN QUAN

Điều 18. Trách nhiệm của Lãnh đạo Cục

1. Cục trưởng chịu trách nhiệm của người đứng đầu về công tác bảo đảm an ninh mạng trước Bộ trưởng và pháp luật.

2. Phó Cục trưởng phụ trách an ninh mạng chịu trách nhiệm:

a) Chỉ đạo, đôn đốc các đơn vị thuộc Cục tuyên truyền, phổ biến, thực hiện và tuân thủ các quy định tại Quy chế này.

b) Chỉ đạo, phân công các đơn vị vận hành các hệ thống thông tin triển khai công tác bảo đảm an ninh mạng trong tất cả các công đoạn liên quan đến hệ thống thông tin.

c) Chủ trì công tác thẩm định, trình phê duyệt, phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng theo quy định tại Nghị định số 331/2026/NĐ-CP.

d) Chỉ đạo công tác đào tạo, bồi dưỡng, tăng cường năng lực cho bộ phận chuyên trách về an ninh mạng và các cá nhân đảm nhiệm công tác an ninh mạng.

Điều 19. Trách nhiệm của các đơn vị thuộc Cục

1. Tổ chức triển khai thực hiện trách nhiệm được giao trong Quy chế này tại đơn vị.

2. Xây dựng, triển khai Quy chế bảo đảm an ninh mạng cho các hệ thống thông tin trong phạm vi quản lý, bảo đảm phù hợp với Quy chế này và các yêu cầu cụ thể của đơn vị.

3. Thực hiện việc quản lý trang thiết bị công nghệ thông tin và công chức, viên chức, người lao động theo Điều 10, Điều 12 và Điều 13 của Quy chế này.

4. Xác định các yêu cầu và trách nhiệm cụ thể của bộ phận, cán bộ, nhân viên trong việc bảo đảm an ninh mạng cho từng vị trí phân công.

5. Thực hiện đúng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản liên quan đến hệ thống thông tin đối với các cá nhân do đơn vị quản lý. Thường xuyên rà soát, kiểm tra quyền truy cập vào các hệ thống thông tin đối với tất cả cán bộ, công chức, viên chức và người lao động bảo đảm quyền truy cập phù hợp với nhiệm vụ được giao.

6. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an ninh mạng; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng đến toàn thể công chức, viên chức và người lao động tại đơn vị.

Điều 20. Trách nhiệm của Phòng An toàn thông tin

1. Thực hiện trách nhiệm của đơn vị chuyên trách về an ninh mạng theo quy định tại Điều 32 Nghị định 331/2026/NĐ-CP, Quy chế này và các nhiệm vụ do Lãnh đạo Cục phân công.

2. Xây dựng kế hoạch, báo cáo về an ninh mạng của Cục.

3. Theo dõi, đôn đốc, giám sát, kiểm tra và báo cáo Cục việc thực hiện Quy chế này tại các đơn vị thuộc Cục.

4. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về an ninh mạng; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng tại Cục, Bộ lồng ghép trong các chương trình hội nghị, tập huấn, hội thảo về ứng dụng công nghệ thông tin và chuyển đổi số của ngành nông nghiệp và môi trường.

5. Đôn đốc, giám sát thực hiện bảo đảm an ninh mạng cho các hệ thống thông tin, cơ sở dữ liệu dùng chung, trọng yếu của Cục, Bộ.

6. Tổ chức rà soát định kỳ hàng năm để kiểm tra tính phù hợp của Quy chế này với các quy định của pháp luật về an ninh mạng và các quy định, tiêu chuẩn liên quan; báo cáo Lãnh đạo Cục về việc sửa đổi, bổ sung Quy chế trong trường hợp cần thiết.

Điều 21. Trách nhiệm của đơn vị vận hành Trung tâm dữ liệu của Bộ do Cục quản lý

1. Trung tâm Hạ tầng số thực hiện trách nhiệm là đơn vị vận hành và bảo đảm an ninh mạng cho hạ tầng Trung tâm dữ liệu của Bộ; giám sát bảo đảm an ninh mạng cho các hệ thống thông tin do Cục quản lý tại Hà Nội.

2. Trung tâm Dữ liệu thông tin phía Nam thực hiện trách nhiệm vận hành và bảo đảm an ninh mạng cho hạ tầng Trung tâm dữ liệu của Bộ; giám sát bảo đảm an ninh mạng cho các hệ thống thông tin do Cục quản lý tại TP. Hồ Chí Minh và thành phố Cần Thơ.

3. Trung tâm Hạ tầng số là đầu mối tiếp nhận và phối hợp khắc phục sự cố an ninh mạng trong Cục, tổng hợp danh sách sự cố và tình trạng khắc phục gửi Phòng An toàn thông tin để theo dõi, tổng hợp.

Điều 22. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 33 Nghị định 331/2026/NĐ-CP, Quy chế này và các nhiệm vụ do Cục phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý mạng; quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an ninh mạng trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 23. Trách nhiệm cá nhân

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: Thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước

pháp luật và Lãnh đạo Cục về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Công chức, viên chức, người lao động của Cục, các đơn vị thuộc Cục và các đơn vị khác thuộc đối tượng áp dụng của Quy chế có trách nhiệm: tuân thủ Quy chế; thông báo các dấu hiệu mất an ninh mạng cho đơn vị, bộ phận chuyên trách về an ninh mạng của đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu quan trọng hoặc dữ liệu mật của ngành nông nghiệp và môi trường do không tuân thủ Quy chế.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 24. Kinh phí thực hiện

Kinh phí bảo đảm an ninh mạng được lấy từ nguồn ngân sách nhà nước dự toán hàng năm của Cục Chuyển đổi số theo quy định.

Căn cứ vào kế hoạch hàng năm, các đơn vị liên quan có trách nhiệm đề xuất dự toán cho các hoạt động bảo đảm an ninh mạng gửi Phòng Tài chính – Thống kê để tổng hợp, thẩm định, trình cấp có thẩm quyền phê duyệt.

Điều 25. Chế độ báo cáo

1. Các loại báo cáo về an ninh mạng gồm:

a) Báo cáo công tác khắc phục mã độc, lỗ hổng, điểm yếu và triển khai cảnh báo an ninh mạng;

b) Báo cáo hoạt động giám sát của chủ quản hệ thống thông tin;

c) Báo cáo đột xuất theo yêu cầu của Phòng An toàn thông tin, Lãnh đạo Cục.

2. Trách nhiệm lập, phê duyệt báo cáo

a) Các đơn vị thuộc Cục có trách nhiệm lập báo cáo theo nội dung quy định tại khoản 1 Điều này gửi Phòng An toàn thông tin.

b) Phòng An toàn thông tin chịu trách nhiệm tập hợp, tổng hợp báo cáo của các đơn vị, trình Lãnh đạo Cục phê duyệt, gửi Lãnh đạo Bộ và các cơ quan quản lý nhà nước về an ninh mạng.

Điều 26. Khen thưởng, kỷ luật

1. Kết quả thực hiện Quy chế này là một trong những tiêu chí đánh giá kết quả thực hiện hàng năm của cá nhân, đơn vị đồng thời là tiêu chí bắt buộc để xem xét tình hình khen thưởng và danh hiệu thi đua đối với các tổ chức, cá nhân.

2. Đơn vị, cá nhân vi phạm Quy chế này và các quy định khác của pháp luật về an ninh mạng, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật; nếu vi phạm gây thiệt hại đến tài sản, thiết bị, thông tin, dữ liệu thì chịu trách nhiệm bồi thường theo pháp luật hiện hành.

Điều 27. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị thuộc Cục có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức, người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2. Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị phản ánh về Phòng An toàn thông tin để tổng hợp, trình Cục trưởng xem xét, sửa đổi, bổ sung Quy chế./.